Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

Sunday, January 15, 2006

Laws for the mind police

"Cybercrime" statutes often create a very vague and broad prohibition (e.g. against "annoy[ing]" someone anonymously or pseudonymously, against "unauthorized" access to a computer, etc.) For example, a bill recently hidden in a U.S. federal budget authorization and signed by the President makes it a crime for an Internet user to send or post a message on the Internet "without disclosing his identity and with intent to annoy."

Declan McCullough wrote this good layman's analysis of the new anti-Internet-annoyance law. Declan's analysis has, however, been roundly criticized by legal scholars based in Washington D.C.

Scholars who fear the Internet or favor arbitrary government power, or who out of excess love of authority wish to justify laws enacted from such motivations, typically give three kinds of arguments to justify these despicable mind police laws:

(1) Don't worry about it, it was already the law. For example, the above anti-annoyance law already applied to "telecommunications devices." But if it's already the law, how is it any less useful to inform people that a law that already exists, but that they were probably not aware of it or at least of its implications, than to inform them of a new law? And if it's already the law, why did whoever put the language into a bill feel the need to change it? Eugene Volokh's markup of the bill's language (see below) demonstrates that, contrary to what some others have argued, the recent anti-annoyance bill has indeed changed the law for the Internet.

(2) Dont' worry, "intent to X" is far more serious than the mere act with an effect of X and doesn't reach nearly as many people. Unauthorized access is not per se culpable, but intent to gain unauthorized access is. Being annoying is not culpable but intent to annoy is. This avoids a basic question -- why should a state of mind be criminally culpable just because one of the results intended by that state of mind is a minor problem that occur quite often many people's or business's lives, such as unauthorized access or annoyance? A law that proscribes a state of mind intending to commit the act implies that the result itself is so extreme that the criminal law should reach through the wires to reach it. But Internet users are annoyed hundreds of millions of times a day. There are millions of innoccous but unauthorized accesses per day. These are nowhere close to the extremity of result required to render intending that result to be a criminal state of mind. Furthermore, the law does not say "sole intent" to annoy. This means that one can intend multiple things by an Internet message, but as long as one of those intentions, however minor, was to annoy a potential reader of the message, then under the plain meaning of the statute you are guilty of a crime. Under the plain meaning of the new law, if you intend to mildly annoy *and* entertain *and*inform readers under a pseudonym, you a guilty of a crime. If you intend to entertain and inform all readers and intend to annoy just a few potential readers (as has often occurred with politically valuable speech, for example with much pseudonymous speech in and related to *The Federalist Papers*), you are guilty of a crime, under the properly interpreted

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

statute.

(3) Don't worry, the courts won't really take the language seriously. Daniel Solove, for example, argues "I'm certain that this [identity requirement] provision will be read narrowly to apply to individuals who intend to persistently or menacingly harass a person." How can he be so certain? Solove is putting a very large degree of trust in the courts to read a statute in a way that is very different from the plain meaning of the statute and in a way that violates a basic canon of legal interpretation, namely that when Congress adds a phrase to a list it must mean something that the other members of the list did not mean. Congress must have added "annoy" because they meant to cover more states of mind than just intentions to "abuse, threaten, or harass." Nor does Solove explain why a court would be compelled by law, rather than merely biased by an inclination to justice, to read the statute narrowly if the court feels strongly that it should not. For example, the court may find the political opinions expressed in the speech beyond their pale and apply normal plain-meaning and common canon interpretation instead of Solove's method of ignoring the text. Orin Kerr cites the First Amendment as a reason a court would read the statute narrowly, but doesn't explain why a court should not more properly apply the substantial overbreadth doctrine and throw out the entire clause, or at least the entire word "annoy," as facially unconstitutional. Kerr by making this argument implies that there are many kinds of mind police prosecutions against an "intent to annoy" that fall short of an "intent to...harass" that he expects courts to find constitutional. This implies the result Eugene Volokh pointed out using a different line of reasoning, that courts would be carving out a new exception to the First Amendment for online and phone speech. Finally, neither Kerr nor Solove address the severe damage done to our legal system in terms of notice and rule of law when courts must throw plain meaning and standard canons of interpretation out the window in order to do justice.

Unless we can trust the courts to severely restrict their scope or find them unconstitutional, these statutes are open invitations for prosecutors to attack almost any variety of Internet activity they don't like and that they think they can convince a judge or jury not to like. Cybercrime statutes are generally not "laws" in the sense of "rule of law," but invitations to arbitrary bureaucratic dominion over almost any kind of Internet behavior, checked only by judges who wish to throw proper legal interpretation out the window (and, in the U.S., checked by juries).

Here's the actual language (via Eugene Volokh) of the anti-pseudonymous-annoyance clause, with snuck-in revision that makes it apply to the Internet underlined:

> 47 U.S.C. § 223(a)(1)(C): Whoever ... in interstate or foreign communications ... makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications....
>
> (h)(1) The use of the term “telecommunications device” in this section --
> (A) shall not impose new obligations on broadcasting station licensees and cable operators covered by obscenity and indecency provisions elsewhere in this chapter; and
> (B) does not include an interactive computer service [= any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions].; and
> <u>(C) in the case of subparagraph (C) of subsection (a)(1), includes any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet ....</u>

Posted by Nick Szabo at 7:58 AM

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ► November (7)
  - ► October (15)
  - ► September (15)
  - ► August (20)
  - ► July (5)
  - ► June (10)
  - ► May (4)
  - ► April (3)
  - ► March (11)
  - ► February (10)
  - ▼ January (26)
    - Death by government
    - Two views of Tiananmen Square
    - Free banker to be on Federal Reserve Board?
    - E-gold challenges forfeiture
    - History, property, and security -- update
    - BlackBerry appeal denied
    - Estimating the value of favors
    - Long distance trade in pre-Roman northern Europe

1 comment:

Anonymous said...

We have unauthorized access laws because hiring a corporate lobbyist is cheaper and more fun than hiring computer security people or ensuring that the corporation buys their software from a vendor that cares about security (which would exclude Microsoft for starters). The tax money to pay to enforce these laws -- er, to try to enforce these laws, since they mostly go without enforcement, thank God -- is far higher than the cost of either security people or secure software. But the corporate lobbyists and their Congressional friends don't care about that; they are not footing the bill. It's suckers like you and me that foot the bill for all the time wasted tracking down crackers, alleged crackers, false leads, and people the cops want to harrass for entirely different reasons.

8:44 AM

Post a Comment

Newer Post Home Older Post

Subscribe to: Post Comments (Atom)

From contracts to money

Google challenges sweeping subpoena for search eng...

What data is on your hotel card key?

Some recent patent news

Professionals sue to stop illegal NSA surveillance...

Trial by ordeal

Laws for the mind police

Multiparty secure computation

More from former NSA spy

Warrantless NSA spying illegal -- more scholars an...

NSA spy doffs his mask

Cowen on currency

Schneier on Project Shamrock

"History and the Security of Property"

E-gold woes

"Imaginary" property

Defensible positions

Shells

► 2005 (44)

Simple theme. Powered by Blogger.